FACTS ON PAC FIELDS AND STABLE FIELDS(Model Theory of fields and its applications)

AUTHOR(S):

YONEDA, IKUO

数理解析研究所講究録
1515巻 2006年 52-62

FACTS ON PAC FIELDS AND STABLE FIELDS

東海大学理学部数学科 米田郁生 (IKUO YONEDA)
DEPARTMENT OF MATHEMATICS, TOKAI UNIVERSITY

1. INTRODUCTION

In this exposition, we show the following two fact.

- Duret's result: Any PAC non-separably closed field has the independent property. [D]
- Scanlon's result : Any infinite stable field of characteristic $p > 0$ is separably closed in finite extensions of degree divided by p, and contains $\overline{\mathbb{F}_p}$. [S]

As the independence proerty implies unstable, any PAC stable field is separably closed. (It is still open whether stable fields are separably closed or not.) This note is organaized as follows. In section 2, we review classical field theory and the definition of PAC fields. For showing Duret's result, we consider separable extensions of PAC fields, in section 3, Kummer extension case, in section 4, Artin-Schreier extension case. Combining Propositions in section 3,4, we show Duret's result in section 5. Scanlon's results are in section 6.

2. BASIC FACTS ON VARIETIES AND FIELDS

Let k be a subfield of K, and let $\tilde{k}$ be the smallest algebraically closed field containing k. When $k \subset k', k''$ are fields, and k' and k'' are linearly over k, we write $k' \mathop{\downarrow}_k k''$.

We begin with the basic fact on galois extensions.

Fact 2.1. *Suppose that k'/k is galois extension and k''/k is an extension. Then $k' \mathop{\downarrow}_k k''$ iff $k' \cap k'' = k$.*

Proof. Suppose that $k' \cap k'' = k$. To show the linear disjointness, we may assume that $k' = k(a)$. Let $p(x) = \Pi_{1 \leq i \leq n}(x - a_i)$ be the minimal polynomial of a over k, where $[k' : k] = n$. Then $a_i \in k'$ because k'/k galois. And we may assume that the minimal polynomial $q(x)$ of a over k'' is of form $\Pi_{1 \leq i \leq m}(x - a_i)$, where $m = [k''(a) : k'']$. As $a_i \in k' \cap k''(i = 1, \ldots m)$, $q(x) \in k[x]$, $p(x) = q(x)$ and $[k(a) : k] = [k''(a) : k'']$ follow. □

We summarize the relation between fields and Zariski closed sets.

Fact 2.2. *Let V be a k-irreducible Zariski closed set.*

(1) *V is defined over k iff $k(V) \perp_k k^{1/p^\infty}$.*
(2) *V is absolutely irreducible iff $k(V) \cap k_s = k$ iff $k(V) \perp_k k_s$.*
(3) *V is an affine variety over k iff $k(V)$ is a regular extension of k.*

Proof. Let $\bar{a} \in V$ be generic over k. So $k(V)(= k[\bar{X}]/I(V) \cap k[\bar{X}]) = k(\bar{a})$ and $I(V) = I(\bar{a}/\tilde{k})$.
(1): As V is definable over k in ACF, by considering the definition field, we see that V is defined over k^{1/p^∞}. So, $I(V)$ is generated by $I(\bar{a}/k^{1/p^\infty})$. Now, V is defined over k iff $I(V)$ is generated by $I(\bar{a}/k)$ iff $I(\bar{a}/k^{1/p^\infty})$ is generated by $I(\bar{a}/k)$ iff $k(\bar{a}) \perp_k k^{1/p^\infty}$, as desired.
(2): The following are equivalent.
(a) V is absolutely irreducible. (b) $I(\bar{a}/k^{1/p^\infty})$ generates $I(\bar{a}/\tilde{k})$.
(c) $k^{1/p^\infty}(\bar{a}) \perp_{k^{1/p^\infty}} \tilde{k}$.

Claim. *(c)$\Rightarrow k(\bar{a}) \cap k_s = k \Rightarrow$ (a).*

First implication: $k \subseteq k(V) \cap k_s \subseteq k^{1/p^\infty} \cap k_s = k$. Second implication :
By Fact 2.1, $k(\bar{a}) \perp_k k_s$, so $I(\bar{a}/k)$ genarates $I(\bar{a}/k_s)$. Let $\bar{b} \in V$ be k-generic. Then $I(\bar{a}/k_s) = I(\bar{b}/k_s)$ follows, so V is invariant over galois actions, as desired.
(3): ($\Rightarrow$) As V is defined over k_s and $\tilde{k} = (k_s)^{1/p^\infty}$, $k_s(V) \perp_{k_s} \tilde{k}$ by (1). By (2), $k(V) \perp_k k_s$, so $k(V) \perp_k \tilde{k}$ follows. ($\Leftarrow$) As $k(V) \perp_k \tilde{k}$ and $k(V) \perp_k k_s$, we see $k(V) \perp_k k^{1/p^\infty}$. By (1) (2), the conclusion follows. □

Fact 2.3. *Let K/k be separable extension of degree n. Let V be an affine variety over K. Then there exists an affine variety $\tilde{V}$ over k such that*

(1) *$\tilde{V} \simeq_L V^n$, where L is the galois closure of K over k,*
(2) *there is a bijeciton between $V(K)$ and $\tilde{V}(k)$.*

Proof. Let $b_1, b_2, \ldots, b_n$ be a linear bases of K over k and let $f_1, \ldots, f_m \in K[X_1, \ldots, X_l]$ be generators of $I(V) \cap K[X_1, \ldots, X_l]$. We prepare $l \times n$-many variables $(Y_{i,j})_{1 \le i \le l, 1 \le j \le n}$. Let $g_i \in K[Y_{1,1}, \ldots, Y_{l,n}]$ be the polynomial replaced f_i by $X_i = \Sigma_{1 \le j \le n} Y_{i,j} b_j$. As b_j are bases, there exist $g_{i,j} \in k[Y_{1,1}, \ldots, Y_{l,n}]$ such that $g_i = \Sigma_{1 \le j \le n} g_{i,j} b_j$. Let $\tilde{V}$ be the k-Zariski closed set defined by the ideal generated by $\{g_{i,j} : 1 \le i \le m, 1 \le j \le n\}$. Note that if $(a_{1,1}, \ldots, a_{l,n}) \in \tilde{V}(k)$, then $(\Sigma_{1 \le j \le n} a_{1,j} b_j, \ldots, \Sigma_{1 \le j \le n} a_{l,j} b_j) \in V(K)$.
As K/k is finite and separable, there exists $\alpha \in K$ such that $k(\alpha) = K$. Let $\alpha_i (1 \le i \le n)$ be all the k-conjugates of $\alpha = \alpha_1$ and let $\sigma_i \in \mathrm{Aut}(\tilde{k}/k)$ be such that $\sigma_i(\alpha) = \alpha_i$. Then $L = k(\alpha_1, \ldots, \alpha_n)$ is the galois closure of K over k.

Claim. $\tilde{V} \simeq_L \sigma_1(V) \times \ldots \times \sigma_n(V)$.

Let $B = (\sigma_j(b_k))_{1\leq j,k\leq n} \in M_n(L)$. Put $\begin{pmatrix} x_{1i} \\ x_{2i} \\ \cdot \\ \cdot \\ \cdot \\ x_{ni} \end{pmatrix} = B \cdot \begin{pmatrix} y_{1i} \\ y_{2i} \\ \cdot \\ \cdot \\ \cdot \\ y_{ni} \end{pmatrix}$ $(i = 1, \ldots, n)$, where $(y_{11}, \cdots, y_{ln}) \in \tilde{V}$.
As $x_{ji} = \Sigma_{1\leq k\leq n} y_{ki}\sigma_j(b_k)$, $(x_{j1}, \ldots, x_{jl}) \in \sigma_j(V)$.
Now, we show that $B \in GL_n(L)$: If not, there exists $c_1, \ldots, c_n \in \tilde{k}$ such that $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$ and $\Sigma_{1\leq i\leq n} c_i\sigma_i(b_k)$ for any $1 \leq k \leq n$. Then we have

$$\Sigma_{1\leq i\leq n} c_i\sigma_i|K = 0.$$

For any $a = \Sigma_{1\leq k\leq n} a_k b_k$, where $a_k \in k$,
$(\Sigma_{1\leq i\leq n} c_i\sigma_i)(\Sigma_{1\leq k\leq n} a_k b_k) = \Sigma_{1\leq i\leq n}\Sigma_{1\leq k\leq n} c_i a_k\sigma_i(b_k) = \Sigma_{1\leq k\leq n} a_k \Sigma_{1\leq i\leq n} c_i\sigma_i(b_k) = 0$.
Recall Dedekind Theorem: Let K, K' be fields and $\sigma_i : K \to K'$ be isomorphisms. Suppose that $\Sigma_{1\leq i\leq n} a_i\sigma_i|K = 0$ and $a_i \in K'$. Then $a_1 = \cdots = a_n = 0$.
The proof of Dedekind Theorem: Othewise, take $0 \neq a_1, \ldots, a_n \in K'$ such that $\Sigma_{1\leq i\leq n} a_i\sigma_i|K = 0$ and n is minimal. Clearly $n \geq 2$. We have two equations as follows. $\Sigma_{1\leq i\leq n} a_i\sigma_i(a)\sigma_i(b) = 0, \Sigma_{1\leq i\leq n} a_i\sigma_i(a)\sigma_n(b) = 0$ for any $a, b \in K$. Take $b \in K$ such that $\sigma_1(b) \neq \sigma_n(b)$. Put $b_i = a_i(\sigma_i(b) - \sigma_n(b))$. Then $\Sigma_{1\leq i\leq n-1} b_i\sigma_i(a) = 0$ and $b_1 \neq 0$, a contradiction.
So, by Dedekind Theorem, $c_1 = \ldots = c_n = 0$, a contradiction.

As $B \in GL_n(L)$, B gives an injection from $\tilde{V}$ to $\sigma_1(V) \times \ldots \times \sigma_n(V)$. Note that B sends $\tilde{V}(k)$ to $\sigma_1(V(K)) \times \ldots \times \sigma_n(V(K))$, so there is an injection from $\tilde{V}(k)$ to $V(K)$.

Finally, we check its surjectivity. Put $\begin{pmatrix} y_{1i} \\ y_{2i} \\ \cdot \\ \cdot \\ \cdot \\ y_{ni} \end{pmatrix} = B^{-1} \cdot \begin{pmatrix} x_{1i} \\ x_{2i} \\ \cdot \\ \cdot \\ \cdot \\ x_{ni} \end{pmatrix}$, where $(x_{11}, \ldots, x_{ln}) \in \sigma_1(V) \times \ldots \times \sigma_n(V)$. Put $e_{ij} = g_{ij}(y_{11}, \ldots, y_{ln})$. Then We show $e_{ij} = 0$ for $1 \leq i \leq m, 1 \leq j \leq n$.

As $Q_i(Y_{11}, \ldots, Y_{ln}) = \Sigma_{1\leq j\leq n} q_{ij}b_j$, $\sigma(Q_i) = \Sigma_{1\leq j\leq n} q_{ij}\sigma(b_j)$. So, $\Sigma_{1\leq j\leq n} e_{ij}\sigma_k(b_j) = \sigma_k(Q_i)(y_{11}, \ldots, y_{ln}) = \sigma_k(P_i)(x_{k1}, \ldots, x_{kl}) = 0$. (By $x_{ki} = \Sigma_{1\leq j\leq n} y_{ij}\sigma_k(b_j)$ and the definition of Q_i.)

Therefore $B \begin{pmatrix} e_{i1} \\ \cdot \\ \cdot \\ \cdot \\ e_{in} \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$. As $B \in GL_n(L)$, the conclusion follows.

By considering points under $Gal(L/k)$, we see that B maps $\tilde{V}(k)$ to $V(K)$. □

Definition 2.4. We say that a field k is PAC (pseudo algebraically closed), if any absolutely irreducible k-affine variety has a k-rational point.

Proposition 2.5. *Let k be PAC, and let K/k be algebraic separable extension. Then K is PAC.*

Let V be absolutely irreducible K-affine variety. By considering the definition field of V, we may assume K/k is finite. By Fact 2.3, there exists an k-affine variety $\tilde{V} \simeq_L V^n$, where $n = deg(K/k)$ and L is the galois closure. As V is absolutely irreducible, so is $\tilde{V}$. As k is PAC, so $\tilde{V}(k) \neq \emptyset$. By Fact 2.3 again, $V(K) \neq \emptyset$ follows. □

Lemma 2.6. *Let k be PAC, and let I be an absolutuly prime ideal in $k[X_1, \ldots, X_n]$. Suppose that $g(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n] - I$. Then there is $\bar{a} \in k$ such that $\bar{a} \in Z(I) - Z(g)$.*

Proof. Let $K = Q(k[X_1, \ldots, X_n]/I) = k(\bar{X}_1, \ldots, \bar{X}_n)$, where $\pi : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/I$ and $\pi(X_i) = \bar{X}_i$. We define $\varphi : k[X_1, \ldots, X_n, Y] \to K$ as follows. $\varphi|k = \mathrm{id}_k, \varphi(X_i) = \bar{X}_i$ and $\varphi(Y) = \dfrac{1}{\pi(g(X_1, \ldots, X_n))}$. $k[\bar{X}_1, \ldots, \bar{X}_n] \subset R := k[X_1, \ldots, X_n, Y]/\ker(\varphi) \cong \mathrm{im}(\varphi) \subset K$, so $Q(R) = K$. As K/k is a regular extension, $\ker(\varphi)$ is absolutely prime. As k is PAC, there is $\bar{a} \in k$ such that $\bar{a} \in Z(\ker(\varphi))$. Then $Y \cdot g(X_1, \ldots, X_n) - 1 \in \ker(\varphi)$ and $I \subset \ker(\varphi)$ and $g(\bar{a}) \neq 0$, so the conclusion follows. □

The next is an easy lemma of basic ring theory, and will be used in this note.

Lemma 2.7. *Let R be an integral domain, and let $k = Q(R)$ be the quotient field. Let $f_1(X), \ldots f_n(X) \in R[X]$ be monic non-constant polynomials. Suppose that $[k(\alpha_1, \ldots, \alpha_n) : k] = \Pi_{i=1}^n deg(f_i)$, where $f_i(\alpha_i) = 0$. THEN $I = \langle f_1(X_1), \ldots, f_n(X_n) \rangle_{R[X_1, \ldots, X_n]}$ is a prime ideal and $I \cap R = \{0\}$.*

Proof. By our assumption, we see that f_i is irreducible over $k(\alpha_0 = 1, \ldots, \alpha_{i-1})$ for $i = 1, \ldots, n$. Then we have

$$k(\alpha_1, \ldots, \alpha_n) \cong k[X_1, \ldots, X_n]/\langle f_1(X_1), \ldots, f_n(X_n) \rangle_{k[X_1, \ldots, X_n]}.$$

Claim. *$A := R[X_1, \ldots, X_n]/I$ is an integral domain.*

As $A \cong R[X_1]/\langle f_1\rangle \otimes_R \ldots \otimes_R R[X_n]/\langle f_n\rangle$ and each $R[X_i]/\langle f_i\rangle \cong R[\alpha_i]$ is finitely genarated R-module, A is a flat R-module. As $0 \to R \to k$, $0 \to R \otimes_R A \cong A \to k \otimes_R A = k \otimes_R (R[X_1, \ldots, X_n]/\langle f_1(X_1), \ldots, f_n(X_n)\rangle_{R[X_1,\ldots,X_n]}) = k[X_1, \ldots, X_n]/\langle f_1(X_1), \ldots, f_n(X_n)\rangle_{k[X_1,\ldots,X_n]} \cong k(\alpha_1, \ldots, \alpha_n)$, as desired. Let $\varphi : A \hookrightarrow k(\alpha_1, \ldots, \alpha_n)$ be the above monomorphism and let $\pi : R[X_1, \ldots, X_n] \to A$ be tha canonical epimorphism. Then $\varphi \circ \pi | R = \mathrm{id}_R$. For $a \in R \cap I$, $a = (\varphi \circ \pi)(a) = \varphi(0) = 0$. □

3. Arguments on Kummer extensions

In this section, p is a prime number and we consider fields whose characteristics are different from p. We recall the following.

Fact 3.1. (1) *Suppose that k contains the primitive root of unity, and k does not have the solution of $X^p - a \in k[X]$. Let α be the solution of $X^p - a \in k[X]$. Then $X^p - a$ is irreducible, and $k(\alpha)/k$ is a galois extension and $Gal(k(\alpha)/k)$ is cyclic of order p and given by $\alpha \mapsto \alpha\xi_p^i$, where $i = 0, 1, \ldots, p-1$ and ξ_p is the primitive p-th root of unity. So, $Gal(k(\alpha)/k) \cong R_p$, where R_p is the group of the p-th roots of unity.*

(2) *Suppose that $ch(k)$ is prime to n. Suppose that k contains the primitive n-root of unity. If L/k is cyclic of degree n, then L is a Kummer extension.*

Lemma 3.2. *Suppose that k contains the primitive root of unity. Let α_i be the solution of $X^p - a_i \in k[X]$ for $i = 1, \ldots, n$. If $k(\alpha_{<i})$ does not have the solution of $X^p - a_i$ for $i = 1, \ldots, n$, then $k(\alpha_1, \ldots, \alpha_n)/k$ is a galois extension and $Gal(k(\alpha_1, \ldots, \alpha_n)/k) \cong R_p^n$.*

Proof. By Lemma 2.7, we see that $k(\alpha_1, \ldots, \alpha_n)/k$ is a galois extension of degree p^n. And, for any $\sigma \in Gal(k(\alpha_1, \ldots, \alpha_n)/k)$, we have $\dfrac{\sigma(\alpha_i)}{\alpha_i} \in R_p$ for any $i = 1, \ldots, n$. So, the conclusion follows. □

Lemma 3.3. *Suppose that k contains the primitive root of unity, and k is the fraction field of a uniquely factorized domain A. Let $a_i \in A (i = 1, \ldots, n)$ be of form $a_i = g_i^{q_i} h_i$, where g_i is prime, q_i is the exponent of a_i in the prime g_i and $(p, q_i) = 1$. Suppose that g_i are distinct and g_i is not a factor of $a_j (i \neq j)$. Let α_i be a root of $X^p - a_i$. Then $\alpha_i \notin k(\alpha_{<i})$ for $i = 1, \ldots, n$.*

Proof. We show this by induction on the n. For $n = 1$; suppose not, then there exist $a, b \in A$ such that these are prime to each other and

$$a^p = g_1^{q_1} h_1 b^p.$$

So, b must be a unit, in particular, the exponent of a^p in g_i must be q_i, a contradiction.

From n to $n+1$; Let $K' = k(\alpha_1, \ldots, \alpha_{n-1}, \alpha_{n+1})$, then $[K', k] = p^n$ by induction hypothesis. And put $K = k(\alpha_1, \ldots, \alpha_n)$. By way of contradiction, suppose that $\alpha_{n+1} \in K$. Then $K' \subsetneq K$ and $[K, k] = p^n$, so $K = K'$. Let $\sigma \in \mathrm{Aut}(K/k)$ be such that $\sigma(\alpha_i) = \alpha_i (i = 1, \ldots, n-1)$ and $\sigma(\alpha_n) = \xi\alpha_n$ by using induction hypothesis. Let N be such that $\sigma(\alpha_{n+1}) = \xi^N \alpha_{n+1}$. Put

$$\alpha = \alpha_n^{p-N}\alpha_{n+1} \in K.$$

Note that $\sigma(\alpha) = \sigma(\alpha_n)^{p-N}\sigma(\alpha_{n+1}) = \xi^{p-N}\alpha_n^{p-N}\xi^N\alpha_{n+1} = \alpha$.

Claim. *$K = k(\alpha_1, \ldots, \alpha_{n-1}, \alpha)$ follows, so $\sigma = \mathrm{id}_K$, a contradiction.*

We have $\alpha^p = a_n^{p-N}a_{n+1} = g_{n+1}^{q_{n+1}}(g_n^{q_n(p-N)}h_n^{p-N}h_{n+1})$. Put $h = g_n^{q_n(p-N)}h_n^{p-N}h_{n+1}$. Then g_{n+1} is not a factor of h. (Otherwise, g_{n+1} is a factor of h_n^{p-N}, moreover, of a_n.) Let $a'_{n+1} = g_{n+1}^{q_{n+1}}h$. As $k(\alpha_1, \ldots, \alpha_{n-1}, \alpha) \subsetneq K$ and $g_1, \ldots, g_{n-1}$ are not any factor of h, by induction hypothesis, the claim follows. □

Proposition 3.4. *Let $A = \tilde{k}[Y_1, \ldots, Y_m]$. Let $f_i \in k[Y_1, \ldots, Y_m], (i = 1, \ldots, n)$ be of form $f_i = g_i^{q_i}h_i$, where, in A, g_i is prime, q_i is the exponent of a_i in the prime g_i and $(p, q_i) = 1$. Suppose that g_i are distinct and g_i is not a factor of $f_j (i \neq j)$ in A. Then the ideal I generated by $\{X_i^p - f_i : i = 1, \ldots, n\}$ in $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ is absolutely prime, and $I \cap k[Y_1, \ldots, Y_m] = \{0\}$.*

Proof. Note that $K := Q(A) = \tilde{k}(Y_1, \ldots, Y_m)$ contains the primitive p-th root. So, by Lemma 3.3, we have $\alpha_i \notin K(\alpha_{<i})$ for $i = 1, \ldots, n$, where α_i is any root of $X_i^p - f_i$. By Lemma 3.2, $[K(\alpha_1, \ldots, \alpha_n) : K] = p^n$ follows. By Lemma 2.7, the ideal generated by $\{X_i^p - f_i : i = 1, \ldots, n\}$ in $\tilde{k}[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ is prime, so the proposition is proven. □

Proposition 3.5. *Let $k \subset K$. Suppose that k is PAC and contain the primitive p-th root of unity, and there is $\alpha \in k$ such that no roots of $X^p - \alpha$ is in K. Let $(a_i)_{i<\omega}$ be distinct elements of k. Let $\varphi(x, y) \equiv \exists z(z^p = x + y)$. Then for any disjoint finite subsets $I, J \subset \omega$,*

$$K \models \exists x(\bigwedge_{i \in I} \varphi(x, a_i) \wedge \bigwedge_{j \in J} \neg\varphi(x, a_j)).$$

So, $\mathrm{Th}(K)$ has the independence property.

Proof. Let $A = k[(X_i)_{i \in I \cup J}, Y]$ and $\mathfrak{P}$ be the ideal generated by $\{X_i^p - (Y + a_i) : i \in I\} \cup \{X_j^p - \alpha(Y + a_j) : j \in J\}$ in A. By Proposition 3.4, we see that $\mathfrak{P}$ is absolutely prime, and $\mathfrak{P} \cap k[Y] = \{0\}$. So, by PAC of k and 2.6 we see that there exist $(c_i)_{i \in I \cup J} d \subset k$ such that

- $c_i^p - (d + a_i) = 0$ for each $i \in I$
- $c_j^p - \alpha(d + a_j) = 0$ for each $j \in J$
- $d + a_j \neq 0$ for each $j \in J$

So, we have that, for each $i \in I$

$$K \models \varphi(d, a_i).$$

Claim. *This $d \in k$ is the desired element for our statement.*

Suppose not, so there exists $j \in J$ such that $K \models \varphi(d, a_j)$. Thus we can find $c'_j \in K^\times$ such that $c'^p_j - (d + a_j) = 0$. But we have that $c_j^p = \alpha(d + a_j)$. So, we get that $\alpha = (\frac{c_j}{c'_j})^p$ and $\frac{c_j}{c'_j} \in K$, a contradiction. □

4. Arguments on Artin-Schreier extensions

In this section, we consider fields of characteristic p. We recall the following.

Fact 4.1. (1) *Suppose that k does not have the solution of $X^p - X - a \in k[X]$. Let α be the solution of $X^p - a \in k[X]$. Then $X^p - X - a$ is irreducible over k, and $k(\alpha)/k$ is a galois extension and $Gal(k(\alpha)/k)$ is cyclic of order p and given by $\alpha \mapsto \alpha + n$, where $n \in \mathbb{F}_p$. So, $Gal(k(\alpha)/k) \cong \mathbb{F}_p$.*

(2) *If L/k is cyclic of degree p, then L is an Artin-Schreier extension.*

Lemma 4.2. *Let α_i be the solution of $X^p - X - a_i \in k[X]$ for $i = 1, \ldots, n$. If $k(\alpha_{<i})$ does not have the solution of $X^p - X - a_i$ for $i = 1, \ldots, n$, then $k(\alpha_1, \ldots, \alpha_n)/k$ is a galois extension and $Gal(k(\alpha_1, \ldots, \alpha_n)/k) \cong (\mathbb{F}_p, +)^n$.*

Proof. By Lemma 2.7, we see that $k(\alpha_1, \ldots, \alpha_n)/k$ is a galois extension of degree p^n. And, for any $\sigma \in Gal(k(\alpha_1, \ldots, \alpha_n)/k)$, we have $\sigma(\alpha_i) - \alpha_i \in \mathbb{F}_p$ for any $i = 1, \ldots, n$. And, for $\sigma, \tau \in Gal(k(\alpha_1, \ldots, \alpha_n)/k)$, $(\sigma \circ \tau)(\alpha) - \alpha = \sigma((\tau(\alpha) - \alpha) + \alpha) - \alpha = (\tau(\alpha) - \alpha + \sigma(\alpha)) - \alpha$. So, the conclusion follows. □

Lemma 4.3. *Let $a_i, b_i \in k (i = 1, \ldots, n)$ be such that $(a_i)_{i \leq n}$ are linearly independent over $\mathbb{F}_p$. Let α_i be a root of $X^p - X - (a_i Y + b_i)$. Then $\alpha_i \notin k(Y, \alpha_{<i})$ for $i = 1, \ldots, n$.*

Proof. We show this by induction on the n. For $n = 1$; suppose not, then there exist $r, s \in k[Y]$ such that these are prime to each other and

$$(\frac{r}{s})^p - \frac{r}{s} = a_1 Y + b_1.$$

So, we have

$$(a_1 Y + b_1)s^p = r(r^{p-1} - s^{p-1}) \tag{1}$$

$$r^p = s^{p-1}(r + (a_i Y + b_1)s) \tag{2}$$

By (1), $r \mid (a_1 Y + b_1)s^p$, and by (2), $s \mid r^p$. As s, t are prime to each other, we see $s \in k$ and $r \mid (a_1 Y + b_1)$. Since $a_1 Y + b_1 = (\frac{r}{s})^p - \frac{r}{s}$, we see $r \in k[Y] \setminus k$.

As $r \mid (a_1Y + b_1)$, there exists $t \in k^\times$ such that $\frac{r}{s} = t(a_1Y + b_1)$. So, we have $a_1Y + b_1 = (\frac{r}{s})^p - \frac{r}{s} = t^p(a_1^pY^p + b_1^p) - t(a_1Y + b_1)$, contradiction.

From n to $n+1$; Let $K' = k(Y, \alpha_1, \ldots, \alpha_{n-1}, \alpha_{n+1})$, then $[K', k(Y)] = p^n$ by induction hypothesis. And put $K = k(Y, \alpha_1, \ldots, \alpha_n)$. By way of contradiction, suppose that $\alpha_{n+1} \in K$. Then $K' \subsetneq K$ and $[K, k] = p^n$, so $K = K'$. Let $\sigma \in \mathrm{Aut}(K/k(Y))$ be such that $\sigma(\alpha_i) = \alpha_i (i = 1, \ldots, n-1)$ and $\sigma(\alpha_n) = \alpha_n + 1$ by using induction hypothesis. As $(\sigma(\alpha_{n+1}) - \alpha_{n+1})^p - (\sigma(\alpha_{n+1}) - \alpha_{n+1}) = a_1Y + b_1 - (a_1Y + b_1) = 0$, so let $N = \sigma(\alpha_{n+1}) - \alpha_{n+1} \in \mathbb{F}_p$.

Put

$$\alpha = -N\alpha_n + \alpha_{n+1} \in K.$$

Note that $\sigma(\alpha) = -N\sigma(\alpha_n) + \sigma(\alpha_{n+1}) = -N(\alpha_n + 1) + (\alpha_{n+1} + N) = \alpha$.

Claim. *$K = k(\alpha_1, \ldots, \alpha_{n-1}, \alpha)$ follows, so $\sigma = \mathrm{id}_K$, a contradiction.*

We have $\alpha^p - \alpha = (-N)^p\alpha_n^p + \alpha_{n+1}^p + N\alpha_n - \alpha_{n+1} = -N(\alpha_n^p - \alpha_n) + (\alpha_{n+1}^p - \alpha_{n+1}) = -N(a_nY + b_n) + (a_{n+1}Y + b_{n+1}) = (-Na_n + a_{n+1})Y + (-Nb_n + b_{n+1})$. On the other hand, $a_1, \ldots, a_{n-1}, -Na_n + a_{n-1}$ are linearly independent over $\mathbb{F}_p$. By induction hypothesis, the claim follows. □

Remark 4.4. In the proof of Lemma 4.3, working over $\tilde{k}[Y]$, we see that $\alpha_i \notin \tilde{k}(Y, \alpha_{<i})$ for $i = 1, \ldots, n$

Proposition 4.5. *Let $a_i, b_i \in k (i = 1, \ldots, n)$ be such that $(a_i)_{i \le n}$ are linearly independent over $\mathbb{F}_p$. Then the ideal I generated by $\{X_i^p - X_i - (a_iY + b_i) : i = 1, \ldots, n\}$ in $k[Y, X_1, \ldots, X_n]$ is absolutely prime, and $I \cap \tilde{k}[Y] = \{0\}$.*

Proof. Let α_i be the root of $X_i^p - X_i - (a_iY + b_i)$ for $i = 1, \ldots, n$. By Remark ?? and Lemma 4.2, $[\tilde{k}(Y, \alpha_1, \ldots, \alpha_n) : \tilde{k}(Y)] = p^n$ follows. And the statement follows from Fact 2.7. □

Proposition 4.6. *Let $k \subset K$. Suppose that k is PAC, and there is $\alpha \in k$ such that no roots of $X^p - X - \alpha$ is in K. Let $(a_i)_{i<\omega}$ be $\mathbb{F}_p$-linearly independent elements of k. Let $\psi(x, y) \equiv \exists z(z^p - z = x \cdot y)$. Then for any disjoint finite subsets $I, J \subset \omega$,*

$$K \models \exists x(\bigwedge_{i \in I} \psi(x, a_i) \wedge \bigwedge_{j \in J} \neg\psi(x, a_j)).$$

So, $\mathrm{Th}(K)$ has the independence property.

Proof. Let $A = k[(X_i)_{i \in I \cup J}, Y]$ and $\mathfrak{P}$ be the ideal generated by $\{X_i^p - X_i - a_iY : i \in I\} \cup \{X_j^p - X_j - (a_jY + \alpha) : j \in J\}$ in A. By Proposition 4.5, we see that $\mathfrak{P}$ is absolutely prime. So, by PAC of k and 2.6 we see that there exist $(c_i)_{i \in I \cup J} d \subset k$ such that

- $c_i^p - c_i - da_i = 0$ for each $i \in I$
- $c_j^p - c_j - (da_j + \alpha) = 0$ for each $j \in J$

Clearly $d \in k^\times$. Now, we have that, for each $i \in I$

$$K \models \psi(d, a_i).$$

Claim. *This $d \in k$ is the desired element for our statement.*

Suppose not, so there exists $j \in J$ such that $K \models \psi(d, a_j)$. Thus we can find $c_j' \in K$ such that $c_j'^p - c_j' - da_j = 0$. But we have that $c_j^p - c_j - (da_j + \alpha) = 0$. So, we get that $\alpha = (c_j - c_j')^p - (c_j - c_j')$ and $c_j - c_j' \in K$, a contradiction. □

5. Duret's Theorem

We begin with the following classical fact.

Fact 5.1. *Let $k \subset K, L$. Suppose that k is relatively algebraically closed in K, and L is a separable finite extension of k. THEN L is relatively algebraically closed in KL.*

Proof. Let $L = k(a)$. We need to show that if $b \in K(a)$ is algebraic over L, then $b \in L$.

Claim. *b is separable over k, so there exists $c \in K(a)$ such that $k(a, b) = k(c)$.*

The proof of the claim: Let $f \in k[X]$ be the minimal polynomial of a over k. Then f is also irreducible over K and $[K(a) : K] = [k(a) : k]$. (If not, there exists $g \in K[X]$ such that $g \mid f$. But, for any $\sigma \in \mathrm{Aut}(\tilde{K}/k)$ we have $\sigma(g) \mid f$. So, we see that any coefficients in g is in $\tilde{k} \cap K = k$, a contradiction.)
So we see that $K(a)/K$ is finite and separable. In paricular, b is separable over K. By considering the minimal polynomial of b over k, and the above arugument, we see that b is separable over k.

As k is relatively algebraically closed in K, So we have $[k(c) : k] = [K(c) : K], [k(a) : k] = [K(a) : K]$. We have $K(a) = K(c)$, so $[k(a) : k] = [k(c) : k]$ follows. Since $k(a) \subseteq k(c)$, $b \in k(c) = k(a)$, as desired. □

Theorem 5.2. *Let $k \subsetneq K$. Suppose that k is PAC, relatively algebraically closed in K, and non-separably closed. Then $\mathrm{Th}(K)$ has the independence property. In particular, PAC and non-separably closed closed fields have the independence property.*

As k is not separably closed, there exists a galois extension L. Let p be a prime number such that $p \mid [L : k]$. Let k' be the fixed field by a subgroup of $Gal(L/k)$, of order p. So, L/k' is a galois extension of degree p, and k'/k is separable. Let $L = k'(\alpha)$.

- **Kummer case i.e.** $ch(k) \neq p$

To apply Proposition 3.5, we add the primitive p-th root ξ to k'. Let $k_0 = k'(\xi), L_0 = L(\xi)$.

Claim. *L_0/k_0 is a galois extension of degree p.*

Clearly, we have $L_0 = k_0(\alpha)$, so $[L_0 : k_0] \leq p$ follows. As k_0-conjugates of α are k'-conjugates of α, so we see L_0/k_0 is galois. As $Gal(k_0/k') \leq (\mathbb{Z}/p\mathbb{Z})^\times$, we see $[k_0 : k'] \leq p-1$. Then we have

$$[L_0 : k'] = [L_0 : L][L : k'] = [L_0 : L]p = [L_0 : k_0][k_0 : k'].$$

So $p \mid [L_0 : k_0]$, this claim is proven.

By Fact 3.1, there exists $\beta \in k_0$ such that $L_0 = k_0(\beta^{\frac{1}{p}})$. As k'/k and k_0/k' are finite separable, k_0/k is finite separable. Let $k_0 = k(\gamma)$ and Put $K_0 = K(\gamma)$. As k is relatively algebraically closed in K and k_0/k is separable, by Fact 5.1, we see that k_0 is relatively algebraically closed in K_0. In particular, $\beta^{\frac{1}{p}} \notin K_0$. And k_0 is PAC by Proposition 2.5.
Now we can apply Proposition 3.5 with respect to K_0/k_0. So, $\mathrm{Th}(K')$ has the independence property. As K is interpretable in K' by using K-linear base of K', the conclusion follows. So, we finish the Kummer case.

- **Artin-Schreier case, i.e.** $ch(k) = p$.

By Fact 4.1, there exists $\delta \in k'$ such that $L = k'(\delta_0)$, where δ_0 is a root of $X^p - X - \delta$. Let $K' = Kk'$. As k is relatively algebraically closed in K, and k'/k is separable, k' is is relatively algebraically closed in K' and k' is PAC by Fact 5.1 and Proposition 2.5. In particular, $\delta_0 \notin K'$. So, By Proposition 4.6, we see that $\mathrm{Th}(K')$ has the independence property. As K is interpretable in K', the conclusion follows. □

6. Scanlon's result on infinite stable fields

In this section, let K be an infinite stable field of characteristic $p > 0$.

Proposition 6.1. *The Artin-Schereier map $\sigma : x \mapsto x^p - x$ is an onto endomorphism of K. In particular, $K^{p^n} - K = K$ and $\mathbb{F}_{p^n} \subseteq K$ for any $n < \omega$.*

Proof. Our statement is elementary, we assume that K is sufficiently saturated for using compactness theorem. Put

$$k := \bigcap_{n=1}^{\infty} K^{p^n}.$$

Note that k is perfect. For any $y \in K$, $y\sigma(K)$ is a definable subgroup of K^+, defined by $\exists z(y(z^p - z) = x)$. By stability, there exist $a_1(= 1), \ldots, a_n \in k^\times$

such that

$$I := \bigcap_{a \in k^\times} a\sigma(K) = \bigcap_{i=1}^{n} a_i\sigma(K).$$

Claim. *$\sigma(K) \supseteq K^{p^n}$ for some $n < \omega$.*

Let $G \leq (K^\times)^{n+1}$ be an affine additive subgroup over k, defined by

$$(x_1, \ldots, x_n, y) \in G \Leftrightarrow \bigwedge_{i=1}^{n} y = a_i(x_i^p - x_i).$$

Clearly $\dim(G) = 1$. As k is perfect, we see the connected component G^0 is field-theoretically defined over k. So, $G^0 \cong \mathbb{G}_a$ or $\mathbb{GL}_1$, we see $G(k)$ is infinite. In particular, there exist $(x_1, \ldots, x_n, y) \in G(k)$ such that $y \in k^\times$, so $0 \neq y \in \bigcap_{i=1}^{n} a_i\sigma(k)$. As $I \cap k$ is non-zero ideal of k, we see $k \subseteq I \subseteq \sigma(K)$. By compactness, we have $\sigma(K) \supseteq K^{p^n}$ for some $n < \omega$.

Claim. *Let $a \in K$ and let $\alpha \in K$ be such that $a^{p^n} = \alpha^p - \alpha$. Then $\alpha^{p^{-n}} \in K$. Therefore $K = \sigma(K)$.*

Clearly, we have $\sigma(\alpha^{p^{-n}}) = a \in K$, so $K(\alpha^{p^{-n}})/K$ is separable. But, clearly this extension is purely inseparable, so this claim holds. □

Theorem 6.2. (1) $\overline{\mathbb{F}_p} \subseteq K$.

(2) *There is no finite separable extension L of K with $p|[L : K]$.*

Proof. (1): Put $k = K \cap \overline{\mathbb{F}_p}$. By Proposition 6.1, k is infinite. As $k \subseteq \overline{\mathbb{F}_p}$, k is PAC by the Lang-Weil estimates. Note that k is relatively algebraically closed in K. If $\overline{\mathbb{F}_p} \not\subseteq K$, then $\overline{\mathbb{F}_p}$ is a proper separable extension of k. By Theorem 5.2, K would have independence property, this contaradicts stability.
(2): Suppose not. Let M be the Galois closure of L over K. As $[L : K]|[M : K]$, take a subgroup $G \leq \mathrm{Gal}(M/K)$ of order p. Then M is a Galois extension of $\mathrm{Fix}(G)$ of degree p, so an Artin-Schreier extension. On the other hand, $\mathrm{Fix}(G)$ is a finite extension, interpretable in K, so it is stable. This contradicts Proposition 6.1.

References

[D] Jean-Louis Duret, Les corps faiblement algebriquement clos, non separablement clos ont la properiete independance, LMN 834, 1980, pp.136-162

[S] Thomas Scanlon, Infinite stable fields are Artin-Schreier closed, 1999, preprint.

[Z] Zoe Chatzidakis, The'orie des mod'eles des corps finis et pseudo-finis, 1996

E-mail address: ikuo.yoneda@s3.dion.ne.jp